CAYLEY GRAPHS OF ORDER 27p ARE HAMILTONIAN

EBRAHIM GHADERPOUR AND DAVE WITTE MORRIS

ABSTRACT. Suppose G is a finite group, such that |G| = 27p, where p is prime. We show that if S is any generating set of G, then there is a hamiltonian cycle in the corresponding Cayley graph Cay(G; S).

Theorem. If |G| = 27p, where p is prime, then every connected Cayley graph on G has a hamiltonian cycle.

Combining this with results in [1, 2, 6] establishes that:

(0.1) Every Cayley graph on G has a hamiltonian cycle if |G| = kp, where p is prime, $1 \le k < 32$, and $k \ne 24$.

The remainder of the paper provides a proof of the theorem. Here is an outline:

- §1. Preliminaries: known results on hamiltonian cycles in Cayley graphs
- $\S 2$. Assume the Sylow *p*-subgroup of G is normal
 - §2A. A lemma that applies to both of the possible Sylow 3-subgroups
 - $\S 2B$. Sylow 3-subgroup of exponent 3
 - §2C. Sylow 3-subgroup of exponent 9
- §3. Assume the Sylow p-subgroups of G are not normal

1. Preliminaries: known results on Hamiltonian cycles in Cayley graphs

For convenience, we record some known results that provide hamiltonian cycles in various Cayley graphs, after fixing some notation.

Notation [3, $\S 1.1$ and $\S 5.1$]. For any group G, we use:

- (1) G' to denote the commutator subgroup [G, G] of G,
- (2) Z(G) to denote the center of G, and
- (3) $\Phi(G)$ to denote the Frattini subgroup of G.

For $a, b \in G$, we use a^b to denote the *conjugate* $b^{-1}ab$.

Notation. If (s_1, s_2, \ldots, s_n) is any sequence, we use (s_1, s_2, \ldots, s_n) # to denote the sequence $(s_1, s_2, \ldots, s_{n-1})$ that is obtained by deleting the last term.

- (1.1) **Theorem** (Marušič, Durnberger, Keating-Witte [5]). If G' is a cyclic group of prime-power order, then every connected Cayley graph on G has a hamiltonian cycle.
- (1.2) **Lemma** [6, Lem. 2.27]. Let S generate the finite group G, and let $s \in S$. If $\bullet \langle s \rangle \triangleleft G$,

- $Cay(G/\langle s \rangle; S)$ has a hamiltonian cycle, and
- either
 - (1) $s \in Z(G)$, or
 - (2) |s| is prime,

then Cay(G; S) has a hamiltonian cycle.

- (1.3) **Lemma** [1, Lem. 2.7]. Let S generate the finite group G, and let $s \in S$. If
 - $\langle s \rangle \triangleleft G$.
 - \bullet |s| is a divisor of pq, where p and q are distinct primes,
 - $s^p \in Z(G)$,
 - $|G/\langle s \rangle|$ is divisible by q, and
 - $Cay(G/\langle s \rangle; S)$ has a hamiltonian cycle,

then there is a hamiltonian cycle in Cay(G; S).

The following results are well known (and easy to prove):

- (1.4) **Lemma** ("Factor Group Lemma"). Suppose
 - S is a generating set of G,
 - N is a cyclic, normal subgroup of G,
 - (s_1N, \ldots, s_nN) is a hamiltonian cycle in Cay(G/N; S), and
 - the product $s_1 s_2 \cdots s_n$ generates N.

Then $(s_1, \ldots, s_n)^{|N|}$ is a hamiltonian cycle in Cay(G; S).

- (1.5) Corollary. Suppose
 - S is a generating set of G,
 - N is a normal subgroup of G, such that |N| is prime,
 - $s \equiv t \pmod{N}$ for some $s, t \in S \cup S^{-1}$ with $s \neq t$, and
 - there is a hamiltonian cycle in Cay(G/N; S) that uses at least one edge labelled s.

Then there is a hamiltonian cycle in Cav(G; S).

- (1.6) **Definition.** If H is any subgroup of G, then $H \setminus Cay(G; S)$ denotes the multigraph in which:
 - \bullet the vertices are the right cosets of H, and
 - there is an edge joining Hg_1 and Hg_2 for each $s \in S \cup S^{-1}$, such that $g_1s \in Hg_2$.

Thus, if there are two different elements s_1 and s_2 of $S \cup S^{-1}$, such that g_1s_1 and g_1s_2 are both in Hg_2 , then the vertices Hg_1 and Hg_2 are joined by a double edge.

- (1.7) **Lemma** [6, Cor. 2.9]. Suppose
 - S is a generating set of G,
 - H is a subgroup of G, such that |H| is prime,
 - the quotient multigraph $H\backslash Cay(G;S)$ has a hamiltonian cycle C, and
 - C uses some double-edge of $H \setminus Cay(G; S)$.

Then there is a hamiltonian cycle in Cay(G; S).

- (1.8) **Theorem** [7, Cor. 3.3]. Suppose
 - S is a generating set of G,
 - N is a normal p-subgroup of G, and
 - $st^{-1} \in N$, for all $s, t \in S$.

Then Cay(G; S) has a hamiltonian cycle.

- (1.9) Remark. In the proof of our main result, we may assume $p \geq 5$, for otherwise either:
 - |G| = 54 is of the form 18q, where q is prime, so [6, Prop. 9.1] applies, or
 - $|G| = 3^4$ is a prime power, so the main theorem of [8] applies.
 - 2. Assume the Sylow p-subgroup of G is normal

Notation. Let:

- G be a group of order 27p, where p is prime, and $p \ge 5$ (see Remark 1.9),
- S be a minimal generating set for G,
- $P \cong \mathbb{Z}_p$ be a Sylow *p*-subgroup of G,
- w be a generator of P, and
- Q be a Sylow 3-subgroup of G
- (2.1) **Assumption.** In this section, we assume that P is a normal subgroup of G.

Therefore G is a semidirect product:

$$G = Q \ltimes P$$
.

We may assume G' is not cyclic of prime order (for otherwise Theorem 1.1 applies). This implies Q is nonabelian, and acts nontrivially on P, so

$$G' = Q' \times P$$
 is cyclic of order $3p$.

Notation. Since Q is a 3-group and acts nontrivially on $P \cong \mathbb{Z}_p$, we must have $p \equiv 1 \pmod{3}$. Thus, we may choose $r \in \mathbb{Z}$, such that

$$r^3 \equiv 1 \pmod{p}$$
, but $r \not\equiv 1 \pmod{p}$.

Dividing $r^3 - 1$ by r - 1, we see that

$$r^2 + r + 1 \equiv 0 \pmod{p}$$
.

- 2A. A lemma that applies to both of the possible Sylow 3-subgroups. There are only 2 nonabelian groups of order 27, and we will consider them as separate cases, but, first, we cover some common ground.
- (2.2) **Note.** Since Q is a nonabelian group of order 27, and $G = Q \ltimes P \cong Q \ltimes \mathbb{Z}_p$, it is easy to see that

$$Q' = \Phi(Q) = Z(Q) = Z(G) = \Phi(G).$$

- (2.3) Lemma. Assume
 - $s \in (S \cup S^{-1}) \cap Q$, such that s does not centralize P, and
 - $c \in C_Q(P) \setminus \Phi(Q)$.

Then we may assume S is either $\{s, cw\}$ or $\{s, c^2w\}$ or $\{s, scw\}$ or $\{s, sc^2w\}$.

Proof. Since $G/P \cong Q$ is a 2-generated group of prime-power order, there must be an element a of S, such that $\{s,a\}$ generates G/P. We may write

$$a = s^i c^j z w^k$$
, with $0 \le i \le 2, 1 \le j \le 2, z \in Z(Q)$, and $0 \le k < p$.

Note that:

• By replacing a with its inverse if necessary, we may assume $i \in \{0, 1\}$.

- By applying an automorphism of G that fixes s and maps c to cz^j , we may assume z is trivial (since $(cz^j)^j = c^j z^{j^2} = c^j z$).
- By replacing w with w^k if $k \neq 0$, we may assume $k \in \{0, 1\}$.

Thus,

$$a = s^i c^j w^k$$
 with $i, k \in \{0, 1\}$ and $j \in \{1, 2\}$.

Case 1. Assume k = 1. Then $\langle s, a \rangle = G$, so $S = \{s, a\}$. This yields the four listed generating sets.

Case 2. Assume k=0. Then $\langle s,a\rangle=Q$, and there must be a third element b of S, with $b\notin Q$; after replacing w with an appropriate power, we may write b=tw with $t\in Q$. We must have $t\in \langle s,\Phi(Q)\rangle$, for otherwise $\langle s,b\rangle=G$ (which contradicts the minimality of S). Therefore

$$t = s^{i'}z'$$
 with $0 \le i' \le 2$ and $z' \in \Phi(Q) = Z(G)$.

We may assume:

- $i' \neq 0$, for otherwise $b = z'w \in S \cap (Z(G) \times P)$, so Lemma 1.3 applies.
- i' = 1, by replacing b with its inverse if necessary.
- $z' \neq e$, for otherwise s and b provide a double edge in Cay(G/P; S), so Corollary 1.5 applies.

Then $s^{-1}b = z'w$ generates $Z(G) \times P$.

Consider the hamiltonian cycles

$$(a^{-1},s^2)^3, \quad \left((a^{-1},s^2)^3\#,b\right), \quad \text{and} \quad \left((a^{-1},s^2)^3\#\#,b^2\right)$$

in $\operatorname{Cay}(G/\langle z, w \rangle; S)$. Letting $z'' = (a^{-1}s^2)^3 \in \langle z \rangle$, we see that their endpoints in G are (respectively):

$$z''$$
, $z''(s^{-1}b) = z''z'w$, and $z''(s^{-1}b)^s(s^{-1}b) = z''(z')^2w^sw$.

The final two endpoints both have a nontrivial projection to P (since s, being a 3-element, cannot invert w), and at least one of these two endpoints also has a nontrivial projection to Z(G). Such an endpoint generates $Z(G) \times P = \langle z, w \rangle$, so the Factor Group Lemma (1.4) provides a hamiltonian cycle in Cay(G; S).

2B. Sylow 3-subgroup of exponent 3.

(2.4) Lemma. Assume Q is of exponent 3, so

$$Q = \langle \, x,y,z \mid x^3 = y^3 = z^3 = e, \, \, [x,y] = z, \, \, [x,z] = [y,z] = e \, \rangle.$$

Then we may assume:

- (1) $w^x = w^r$, but y and z centralize P, and
- (2) either:
 - (a) $S = \{x, yw\}, or$
 - (b) $S = \{x, xyw\}.$

(2) S must contain an element that does not centralize P, so we may assume $x \in S$. By applying Lemma 2.3 with s = x and c = y, we see that we may assume S is:

$$\{x, yw\}$$
 or $\{x, y^2w\}$ or $\{x, xyw\}$ or $\{x, xy^2w\}$.

But there is an automorphism of G that fixes x and w, and sends y to y^2 , so we need only consider 2 of these possibilities.

(2.5) **Proposition.** Assume, as usual, that |G| = 27p, where p is prime, and that G has a normal Sylow p-subgroup. If the Sylow 3-subgroup Q is of exponent 3, then Cay(G; S) has a hamiltonian cycle.

Proof. We write $\overline{\ }$ for the natural homomorphism from G to $\overline{G} = G/P$. From Lemma 2.4(2), we see that we need only consider two possibilities for S.

Case 1. Assume $S = \{x, yw\}$. For a = x and b = yw, we have the following hamiltonian cycle in Cay(G/P; S):

Its endpoint in G is

Since the walk is a hamiltonian cycle in G/P, we know that this endpoint is in $P = \langle w \rangle$. So all terms except powers of w must cancel. Thus, we need only calculate the contribution from each appearance of w in this expression. To do this, note that if a term w^i is followed by a net total of j appearances of x, then the term contributes a factor of w^{ir^j} to the product. So the endpoint in G is:

$$w^{r^{13}}w^{2r^{12}}w^{r^{10}}w^{r^8}w^{2r^7}w^{r^5}w^{r^3}w^{-r^2}w^{-2}$$
.

Since $r^3 \equiv 1 \pmod{p}$, this simplifies to

$$\begin{split} w^r w^2 w^r w^{r^2} w^{2r} w^{r^2} w w^{-r^2} w^{-2} &= w^{r+2+r+r^2+2r+r^2+1-r^2-2} \\ &= w^{r^2+4r+1} = w^{r^2+r+1} w^{3r} = w^0 w^{3r} = w^{3r}. \end{split}$$

Since $p \nmid 3r$, this endpoint generates P, so the Factor Group Lemma (1.4) provides a hamiltonian cycle in Cay(G; S).

Case 2. Assume $S = \{x, xyw\}$. For a = x and b = xyw, we have the hamiltonian cycle

$$((a,b^2)^3 \#, a)^3$$

in Cay(G/P; S). Its endpoint in G is

$$((ab^2)^3 b^{-1}a)^3 = ((x(xyw)^2)^3 (xyw)^{-1}x)^3 = ((x(x^2y^2w^{r+1}))^3 (w^{-1}y^{-1}x^{-1})x)^3$$

$$= ((y^2w^{r+1})^3 (w^{-1}y^{-1}))^3 = (w^{3(r+1)} (w^{-1}y^{-1}))^3 = (y^{-1}w^{3r+2})^3$$

$$= w^{3(3r+2)}.$$

Since we are free to choose r to be either of the two primitive cube roots of 1 in \mathbb{Z}_p , and the equation 3r+2=0 has only one solution in \mathbb{Z}_p , we may assume r has been selected to make the exponent nonzero. Then the Factor Group Lemma (1.4) provides a hamiltonian cycle in Cay(G; S).

2C. Sylow 3-subgroup of exponent 9.

(2.6) Lemma. Assume Q is of exponent 9, so

$$Q = \langle x, y \mid x^9 = y^3 = e, [x, y] = x^3 \rangle.$$

There are two possibilities for G, depending on whether $C_Q(P)$ contains an element of order 9 or not.

- (1) Assume $C_Q(P)$ does not contain an element of order 9. Then we may assume y centralizes P, but $w^x = w^r$. Furthermore, we may assume:
 - (a) $S = \{x, yw\}, or$
 - (b) $S = \{x, xyw\}.$
- (2) Assume $C_Q(P)$ contains an element of order 9. Then we may assume x centralizes P, but $w^y = w^r$. Furthermore, we may assume:
 - (a) $S = \{xw, y\},\$
 - (b) $S = \{xyw, y\},\$
 - (c) $S = \{xy, xw\}$, or
 - (d) $S = \{xy, x^2yw\}.$

Proof. (1) Since x has order 9, we know that it does not centralize P. But x^3 must centralize P (since x^3 is in G'). Therefore, we may assume $w^x = x^r$ (by replacing x with its inverse if necessary). Also, since $Q/C_Q(P)$ must be cyclic (because $\operatorname{Aut}(P)$ is cyclic), but $C_G(P)$ does not contain an element of order 9, we see that $C_Q(P)$ contains every element of order 3, so y must be in $C_Q(P)$.

Since S must contain an element that does not centralize P, we may assume $x \in S$. By applying Lemma 2.3 with s = x and c = y, we see that we may assume S is:

$$\{x, yw\}$$
 or $\{x, y^2w\}$ or $\{x, xyw\}$ or $\{x, xy^2w\}$.

The second generating set need not be considered, because $(y^2w)^{-1} = yw^{-1} = yw'$, so it is equivalent to the first. Also, the fourth generating set can be converted into the third, since there is an automorphism of G that fixes y, but takes x to xyw and w to w^{-1} .

(2) We may assume $x \in C_Q(P)$, so $C_Q(P) = \langle x \rangle$.

We know that S must contain an element s that does not centralize P, and there are two possibilities: either

- (I) s has order 3, or
- (II) s has order 9.

We consider these two possibilities as separate cases.

Case I. Assume s has order 3. We may assume s = y. Letting c = x, we see from Lemma 2.3 that we may assume S is either

$$\{y, xw\}$$
 or $\{y, x^2w\}$ or $\{y, yxw\}$ or $\{y, yx^2w\}$.

The second and fourth generating sets need not be considered, because there is an automorphism of G that fixes y and w, but takes x to x^2 . Also, the third generating set may be replaced with $\{y, xyw\}$, since there is an automorphism of G that fixes y and w, but takes x to $y^{-1}xy$.

Case II. Assume s has order 9. We may assume s = xy. Letting c = x, we see from Lemma 2.3 that we may assume S is either

$$\{xy, xw\}$$
 or $\{xy, x^2w\}$ or $\{xy, xyxw\}$ or $\{xy, xyx^2w\}$.

The second generating set is equivalent to $\{xy, xw\}$, since the automorphism of G that sends x to x^4 , y to $x^{-3}y$, and w to w^{-1} maps it to $\{xy, (xw)^{-1}\}$. The third generating set is mapped to $\{xy, x^2yw\}$ by the automorphism that sends x to x[x, y] and y to $[x, y]^{-1}y$. The fourth generating set need not be considered, because xyx^2w is an element of order 3 that does not centralize P, which puts it in the previous case.

(2.7) **Proposition.** Assume, as usual, that |G| = 27p, where p is prime, and that G has a normal Sylow p-subgroup. If the Sylow 3-subgroup Q is of exponent 9, then Cay(G; S) has a hamiltonian cycle.

Proof. We will show that, for an appropriate choice of a and b in $S \cup S^{-1}$, the walk

$$(2.8) (a^3, b^{-1}, a, b^{-1}, a^4, b^2, a^{-2}, b, a^2, b, a^3, b, a^{-1}, b^{-1}, a^{-1}, b^{-2})$$

provides a hamiltonian cycle in Cay(G/P; S) whose endpoint in G generates P (so the Factor Group Lemma (1.4) applies).

We begin by verifying two situations in which (2.8) is a hamiltonian cycle:

(HC1) If $|\overline{a}| = 9$, $|\overline{b}| = 3$, and $\overline{a^b} = \overline{a^4}$ in $\overline{G} = G/P$, then we have the hamiltonian cycle

(HC2) If $|\overline{a}| = 9$, $|\overline{b}| = 9$, $\overline{a^b} = \overline{a^7}$, and $\overline{b^3} = \overline{a^6}$ in $\overline{G} = G/P$, then we have the hamiltonian cycle

To calculate the endpoint in G, fix $r_1, r_2 \in \mathbb{Z}_p$, with

$$w^a = w^{r_1}$$
 and $w^b = w^{r_2}$,

and write

$$a = \underline{a}w_1$$
 and $b = \underline{b}w_2$, where $\underline{a}, \underline{b} \in Q$ and $w_1, w_2 \in P$.

Note that if an occurrence of w_i in the product is followed by a net total of j_1 appearances of \underline{a} and a net total of j_2 appearances of \underline{b} , then it contributes a factor of $w_i^{r_1^{j_1}r_2^{j_2}}$ to the product. (A similar occurrence of w_i^{-1} contributes a factor of $w_i^{-r_1^{j_1}r_2^{j_2}}$ to the product.) Furthermore, since $r_1^3 \equiv r_2^3 \equiv 1 \pmod{p}$, there is no harm in reducing j_1 and j_2 modulo 3.

We will apply these considerations only in a few particular situations:

(E1) Assume $w_1 = e$ (so $a \in Q$ and $\underline{a} = a$). Then the endpoint of the path in G is

$$\begin{split} a^3b^{-1}ab^{-1}a^4b^2a^{-2}ba^2ba^3ba^{-1}b^{-1}a^{-1}b^{-2} \\ &= a^3(\underline{b}w_2)^{-1}a(\underline{b}w_2)^{-1}a^4(\underline{b}w_2)^2a^{-2}(\underline{b}w_2)a^2 \\ &\qquad \times (\underline{b}w_2)a^3(\underline{b}w_2)a^{-1}(\underline{b}w_2)^{-1}a^{-1}(\underline{b}w_2)^{-2} \\ &= a^3(w_2^{-1}\underline{b}^{-1})a(w_2^{-1}\underline{b}^{-1})a^4(\underline{b}w_2\underline{b}w_2)a^{-2}(\underline{b}w_2)a^2 \\ &\qquad \times (\underline{b}w_2)a^3(\underline{b}w_2)a^{-1}(w_2^{-1}\underline{b}^{-1})a^{-1}(w_2^{-1}\underline{b}^{-1}w_2^{-1}\underline{b}^{-1}). \end{split}$$

By the above considerations, this simplifies to w_2^m , where

$$m = -1 - r_1^2 r_2 + r_1 r_2 + r_1 + r_2^2 + r_1 r_2 + r_1 - r_1^2 - r_2 - r_2^2$$

= $-r_1^2 r_2 - r_1^2 + 2r_1 r_2 + 2r_1 - r_2 - 1$.

Note that:

- (a) If $r_1 \neq 1$ and $r_2 = 1$, then m simplifies to $6r_1$, because $r_1^2 + r_1 + 1 \equiv 0 \pmod{p}$ in this case.
- (b) If $r_1 \neq 1$ and $r_2 \neq 1$, then m simplifies to $3r_1(r_2+1)$, because $r_1^2 + r_1 + 1 \equiv r_2^2 + r_2 + 1 \equiv 0 \pmod{p}$ in this case.
- (E2) Assume $w_2 = e$ (so $b \in Q$ and $\underline{b} = b$). Then the endpoint of the path in G

$$\begin{split} a^3b^{-1}ab^{-1}a^4b^2a^{-2}ba^2ba^3ba^{-1}b^{-1}a^{-1}b^{-2} \\ &= (\underline{a}w_1)^3b^{-1}(\underline{a}w_1)b^{-1}(\underline{a}w_1)^4b^2(\underline{a}w_1)^{-2}b(\underline{a}w_1)^2b(\underline{a}w_1)^3b(\underline{a}w_1)^{-1}b^{-1}(\underline{a}w_1)^{-1}b^{-2} \\ &= (\underline{a}w_1\underline{a}w_1\underline{a}w_1)b^{-1}(\underline{a}w_1)b^{-1}(\underline{a}w_1\underline{a}w_1\underline{a}w_1\underline{a}w_1)b^2(w_1^{-1}\underline{a}^{-1}w_1^{-1}\underline{a}^{-1}) \\ &\qquad \qquad \times b(\underline{a}w_1\underline{a}w_1)b(\underline{a}w_1\underline{a}w_1\underline{a}w_1)b(w_1^{-1}\underline{a}^{-1})b^{-1}(w_1^{-1}\underline{a}^{-1})b^{-2}. \end{split}$$

By the above considerations, this simplifies to w_1^m , where

$$m = r_1^2 + r_1 + 1 + r_1^2 r_2 + r_1 r_2^2 + r_2^2 + r_1^2 r_2^2 + r_1 r_2^2 - r_1$$
$$- r_1^2 + r_1^2 r_2^2 + r_1 r_2^2 + r_2 + r_1^2 r_2 + r_1 r_2 - r_1 - r_1^2 r_2$$
$$= 2r_1^2 r_2^2 + 3r_1 r_2^2 + r_2^2 + r_1^2 r_2 + r_1 r_2 + r_2 - r_1 + 1.$$

Note that

(a) If $r_1 = 1$ and $r_2 \neq 1$, then m simplifies to $-3(r_2 + 2)$, because $r_2^2 + r_2 + 1 \equiv 0 \pmod{p}$ in this case.

(b) If $r_1 \neq 1$ and $r_2 \neq 1$, then m simplifies to $-r_1r_2 - 2r_1 + r_2 + 2$, because $r_1^2 + r_1 + 1 \equiv r_2^2 + r_2 + 1 \equiv 0 \pmod{p}$ in this case.

Now we provide a hamiltonian cycle for each of the generating sets listed in Lemma 2.6:

- (1a) If $C_Q(P)$ has exponent 3, and $S = \{x, yw\}$, we let a = x and b = yw in (HC1). In this case, we have $w_1 = e$, $r_1 = r$, and $r_2 = 1$, so (E1a) tells us that the endpoint in G is w_2^{6r} .
- (1b) If $C_Q(P)$ has exponent 3, and $S = \{x, xyw\}$, we let a = x and $b = (xyw)^{-1}$ in (HC2). In this case, we have $w_1 = e$, $r_1 = r$ and $r_2 = r^{-1} = r^2$, so (E1b) tells us that the endpoint in G is w_2^m , where

$$m = 3r_1(r_2 + 1) = 3r(r^2 + 1) = 3(r^3 + r) \equiv 3(1 + r) = 3(r + 1) \pmod{p}.$$

- (2a) If $C_Q(P)$ has exponent 9, and $S=\{xw,y\}$, we let a=xw and b=y in (HC1). In this case, we have $w_2=e,\ r_1=1$ and $r_2=r,$ so (E2a) tells us that the endpoint in G is $w_1^{-3(r+2)}$.
- (2b) If $C_Q(P)$ has exponent 9, and $S = \{xyw, y\}$, we let a = xyw and b = y in (HC1). In this case, we have $w_2 = e$ and $r_1 = r_2 = r$, so (E2b) tells us that the endpoint in G is w_2^m , where

$$m = -r_1r_2 - 2r_1 + r_2 + 2 = -r^2 - 2r + r + 2 = -(r^2 + r + 1) + 3 \equiv 3 \pmod{p}.$$

(2c) If $C_Q(P)$ has exponent 9, and $S = \{xy, xw\}$, we let a = xw and $b = (xy)^{-1}$ in (HC2). In this case, we have $w_2 = e$, $r_1 = 1$, and $r_2 = r^{-1} = r^2$, so (E2a) tells us that the endpoint in G is w_1^m , where

$$m = -3(r_2 + 2) = -3(r^2 + 2) \equiv -3(-(r+1) + 2) = 3(r-1) \pmod{p}.$$

(2d) If $C_Q(P)$ has exponent 9, and $S = \{xy, x^2yw\}$, we let a = xy and $b = x^2yw$ in (HC2). In this case, we have $w_1 = e$ and $r_1 = r_2 = r$, so (E1b) tells us that the endpoint in G is w_2^m , where

$$m = 3r_1(r_2 + 1) = 3r(r + 1) = 3(r^2 + r) \equiv 3(-1) = -3 \pmod{p}.$$

In all cases, there is at most one nonzero value of r (modulo p) for which the exponent of w_i is 0. Since we are free to choose r to be either of the two primitive cube roots of 1 in \mathbb{Z}_p , we may assume r has been selected to make the exponent nonzero. Then the Factor Group Lemma (1.4) provides a hamiltonian cycle in Cay(G; S).

- 3. Assume the Sylow p-subgroups of G are not normal
- (3.1) **Lemma.** Assume
 - |G| = 27p, where p is an odd prime, and
 - the Sylow p-subgroups of G are not normal.

Then p = 13, and $G = \mathbb{Z}_{13} \ltimes (\mathbb{Z}_3)^3$, where a generator w of \mathbb{Z}_{13} acts on $(\mathbb{Z}_3)^3$ via multiplication on the right by the matrix

$$W = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Furthermore, we may assume

S is of the form
$$\{w^i, w^j v\}$$
,

where $v = (1, 0, 0) \in (\mathbb{Z}_3)^3$, and

$$(i,j) \in \{(1,0), (2,0), (1,2), (1,3), (1,5), (1,6), (2,5)\}.$$

Proof. Let P be a Sylow p-subgroup of G, and Q be a Sylow 3-subgroup of G. Since no odd prime divides 3-1 or 3^2-1 , and 13 is the only odd prime that divides 3^3-1 , Sylow's Theorem [4, Thm. 15.7, p. 230] implies that p=13, and that $N_G(P)=P$, so G must have a normal p-complement [3, Thm. 7.4.3]; i.e., $G=P\ltimes Q$. Since P must act nontrivially on Q (since P is not normal), we know that it must act nontrivially on $Q/\Phi(Q)$ [3, Thm. 5.3.5, p. 180]. However, P cannot act nontrivially on an elementary abelian group of order 3 or 3^2 , because |P|=13 is not a divisor of 3-1 or 3^2-1 . Therefore, we must have $|Q/\Phi(Q)|=3^3$, so Q must be elementary abelian (and the action of P is irreducible).

Let W be the matrix representing the action of w on $(\mathbb{Z}_3)^3$ (with respect to some basis that will be specified later). In the polynomial ring $\mathbb{Z}_3[X]$, we have the factorization:

(3.2)
$$\frac{X^{13} - 1}{X - 1} = (X^3 - X - 1) \cdot (X^3 + X^2 - 1) \cdot (X^3 + X^2 + X - 1) \cdot (X^3 - X^2 - X - 1).$$

Since $w^{13} = e$, the minimal polynomial of W must be one of the factors on the right-hand side. By replacing w with an appropriate power, we may assume it is the first factor. Then, choosing any nonzero $v \in (\mathbb{Z}_3)^3$, the matrix representation of w with respect to the basis $\{v, v^w, v^{w^2}\}$ is W (the Rational Canonical Form).

Now, let ζ be a primitive 13th root of unity in the finite field GF(27). Then any Galois automorphism of GF(27) over GF(3) must raise ζ to a power. Since the subgroup of order 3 in \mathbb{Z}_{13}^{\times} is generated by the number 3, we conclude that the orbit of ζ under the Galois group is $\{\zeta, \zeta^3, \zeta^9\}$. These must be the 3 roots of one of the irreducible factors on the right-hand side of (3.2). Thus, for any $k \in \mathbb{Z}_{13}^{\times}$, the matrices W^k , W^{3k} , and W^{9k} all have the same minimal polynomial, so they are conjugate under $GL_3(3)$. That is:

(3.3) powers of
$$W$$
 in the same row of the following table are conjugate under $GL_3(3)$:

W, W^3, W^9
W^2, W^5, W^6
W^4, W^{12}, W^{10}
W^7, W^8, W^{11}

There is an element a of S that generates $G/Q \cong P$. Then a has order p, so, replacing it by a conjugate, we may assume $a \in P = \langle w \rangle$, so $a = w^i$ for some $i \in \mathbb{Z}_{13}^{\times}$. From (3.3), we see that we may assume $i \in \{1, 2\}$ (perhaps after replacing a by its inverse).

Now let b be the second element of S, so we may assume $b=w^jv$ for some j. We may assume $0 \le j \le 6$ (by replacing b with its inverse, if necessary). We may also assume $j \ne i$, for otherwise $S \subset aQ$, so Theorem 1.8 applies.

If j = 0, then (i, j) is either (1, 0) or (2, 0), both of which appear in the list; henceforth, let us assume $j \neq 0$.

Case 1. Assume i = 1. Since $j \neq i$, we must have $j \in \{2, 3, 4, 5, 6\}$.

Note that, since W^3 is conjugate to W under $GL_3(3)$ (since they are in the same row of (3.3)), we know that the pair (w, w^4) is isomorphic to the pair $(w^3, (w^3)^4)$ =

 (w^3, w^{-1}) . By replacing b with its inverse, and then interchanging a and b, this is transformed to (w, w^3) . So we may assume $j \neq 4$.

Case 2. Assume i=2. We may assume W^j is in the second or fourth row of the table (for otherwise we could interchange a with b to enter the previous case. So $j \in \{2,5,6\}$. Since $j \neq i$, this implies $j \in \{5,6\}$. However, since W^5 is conjugate to W^2 (since they are in the same row of (3.3)), and we have $(w^2)^3 = w^6$ and $(w^5)^3 = w^2$, we see that the pair (w^2, w^6) is isomorphic to (w^2, w^5) . So we may assume $j \neq 6$.

(3.4) **Proposition.** If |G| = 27p, where p is prime, and the Sylow p-subgroups of G are not normal, then Cay(G; S) has a hamiltonian cycle.

Proof. From Lemma 3.1 (and Remark 1.9), we may assume $G = \mathbb{Z}_{13} \ltimes (\mathbb{Z}_3)^3$. For each of the generating sets listed in Lemma 3.1, we provide an explicit hamiltonian cycle in the quotient multigraph $P \setminus \text{Cay}(G; S)$ that uses at least one double edge. So Lemma 1.7 applies.

To save space, we use $i_1i_2i_3$ to denote the vertex $P(i_1, i_2, i_3)$.

$$\begin{array}{ll} (i,j)=(1,0) & a=w, \quad a^{-1}=w^{12}, \quad b=(1,0,0), \quad b^{-1}=(-1,0,0) \\ \text{Double edge: } 222\to 022 \text{ with } a^{-1} \text{ and } b \end{array}$$

$$(i,j)=(2,0)$$
 $a=w^2$, $a^{-1}=w^{11}$, $b=(1,0,0)$, $b^{-1}=(-1,0,0)$
Double edge: $020\to 220$ with a and b^{-1}

$$(i,j)=(1,2) \quad a=w, \quad a^{-1}=w^{12}, \quad b=w^2(1,0,0), \quad b^{-1}=w^{11}(-1,-1,1)$$
 Double edge: $220\to 022$ with a and b

Acknowledgments. This work was partially supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

References

- [1] S. J. Curran, D. W. Morris, and J. Morris: Hamiltonian cycles in Cayley graphs of order 16p (preprint). http://arxiv.org/abs/1104.0081
- [2] E. Ghaderpour and D. W. Morris: Cayley graphs of order 30p are hamiltonian (preprint). http://arxiv.org/abs/1102.5156
- [3] D. Gorenstein: Finite Groups, Chelsea, New York, 1980.
- [4] T.W. Judson: Abstract Algebra, Virginia Commonwealth University, 2009. ISBN 0-982-40622-3, http://abstract.pugetsound.edu/download.html
- [5] K. Keating and D. Witte: On Hamilton cycles in Cayley graphs with cyclic commutator subgroup. Ann. Discrete Math. 27 (1985) 89-102.

- [6] K. Kutnar, D. Marušič, J. Morris, D. W. Morris, and P. Šparl: Hamiltonian cycles in Cayley graphs whose order has few prime factors, Ars Mathematica Contemporanea (to appear). http://arxiv.org/abs/1009.5795
- [7] D. W. Morris: 2-generated Cayley digraphs on nilpotent groups have hamiltonian paths (preprint). http://arxiv.org/abs/1103.5293
- [8] D. Witte: Cayley digraphs of prime-power order are hamiltonian. J. Comb. Th. B 40 (1986) 107-112.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, Canada

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, Canada